CONTROLLED

Privacy Impact Assessment Template

OFFICE OF CONSERVATORSHIP'S (OCO) SYSTEM TRACKING AND REPORTING (STAR)
(SYSTEM NAME)

3/16/2022
Date

Tasha L. Cooper
Senior Agency Official for Privacy
(202) 649-3091
Tasha.Cooper@fhfa.gov

Guidance for Completing the Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how Personally Identifiable Information (PII) is collected, stored, maintained, and shared. A PIA must be completed when FHFA: 1) develops or procures an Information Technology (IT) system or project that collects, maintains, or disseminates PII that can be used to identify a specific individual; or 2) initiates a new electronic collection of PII for 10 or more members of the public, which includes any information in an identifiable form permitting the physical or online contacting of a specific individual.

System Owners are primarily responsible for completing the PIA with assistance from IT developers, IT security officers, and the Privacy Office.

OVERVIEW SECTION

- Provide a thorough, complete, and clear overview of the System and give the reader the appropriate context to understand the responses. Some questions to consider include:

  - What is the purpose of the System?
  - What will be the primary uses of the System?
  - How will this support the Division's/Office's/Program's mission?

- This section fulfills the E-Government Act's requirement for an introduction to members of the public who may be reading the PIA. PIAs may be made publicly available unless a determination is made to not make the PIA available because publication would raise security concerns and/or reveal classified or sensitive information.

SECTION 1.0 CHARACTERIZATION OF THE INFORMATION

- Identify if the System contains information about individuals, versus statistical, geographical, or financial information, with no link to a name or other identifier, such as, home address, social security number, account number, home, mobile or facsimile telephone number, or personal e-mail address.

- Examples of sources of the information include information that comes from an individual applying for a loan or mortgage, or other forms that an individual completes. A question to consider:

  - Where does the data originate? (e.g., FHFA, Office of Personnel Management, Regulated Entities, other Financial Institutions, or third parties). A third party is usually a non-Federal person or entity, which may be a source of data/information (e.g., a bank, an internet service provider, or a private organization).

- If the System collects information from 10 or more members of the public, ensure that FHFA has received prior approval from OMB to do so or determine whether OMB's approval is needed to collect the information in accordance with the Paperwork Reduction Act. If you are unsure of this last requirement, contact the Office of General Counsel for assistance.

SECTION 2.0 USES OF THE INFORMATION

- Identify the primary uses of the information and how the information supports FHFA's or the Office's/Division's/Program's mission.

- Identify the controls that are in place to ensure the information will be used for the manner for which it was collected. For example, access to the information will be restricted to a limited number of personnel who use the data for their specific program use.

SECTION 3.0 RETENTION

- **The Privacy Act requires an agency to address the retention and disposal of information about individuals. This retention information is published in the Privacy Act System of Record Notice (SORN).**

- The retention periods for data/records that FHFA manages are contained in either the National Archives and Records Administration (NARA) General Records Schedule (GRS) or FHFA's Records Schedule. For the data being created/ maintained in the System, these records schedules are the authoritative sources for this information. For assistance, contact FHFA's Records Management Office.

- Disposing of the data at the end of the retention period is the last state of life-cycle management. Records subject to the Privacy Act have special disposal procedures(e.g. shredding of paper documents).

SECTION 4.0 NOTICE, ACCESS, REDRESS AND CORRECTION

- The Privacy Act requires that "each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. 552a(e)(1).

- Data can be retrieved in a number of ways, but there is usually a personal identifier associated with a record. If the System retrieves information by an individual's name or other unique identifier (e.g. social security number) it is a Privacy Act System and will need a SORN published in the Federal Register. The System may already have a Privacy Act SORN. If you do not have a published SORN, or are unsure whether one exists, contact FHFA's Privacy Office.

- If a name or other unique identifier is not used to retrieve information, it is possible that the System is not a Privacy Act System. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may still be protected from disclosure under the Freedom of Information Act.

- The agency has developed and published an agency specific Privacy Act Rule in the Federal Register (12 CFR Part 1204) that explains how individuals can gain access to information about themselves and correct errors, if appropriate.

- Any employee who knowingly and willfully maintains a System of Records without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to $5,000.

SECTION 5.0 SHARING AND DISCLOSURE

- If you do not know whether or not Systems share data, contact either the business owner of the data, or the IT specialist who knows what interfaces exist between the Systems/applications. As an example, if your System/application shares data with another System/application, ask yourself whether you have access to the data in the interfaced System/application. If so, then your answer is yes, and an explanation is needed.

- Also consider "other" users who may not be obvious as those listed, such as GAO, or FHFA's Office of Inspector General. "Other" may also include database administrators or IT Security Officers. Also include organizations listed in the Privacy Act SORN under the "Routine Use" section when a Privacy Act SORN is required. The more comprehensive the list, the better it is.

- You must first review the SORN to determine whether any information that may come from an existing SORN allows that information to be exchanged and used for these new purposes or uses. There are restrictions on the use and disclosure of information that are set forth in a SORN.

SECTION 6.0 ACCESS AND SECURITY

- Access to data by a user (i.e. employee or contractor personnel) within FHFA is determined on a "need-to-know" basis. This means to authorized employees or contractor personnel who have a need for the information to perform their duties may be granted access to the information. Factors to consider in making this determination include the user's job requirements including supervisory responsibilities.

- The criteria, procedures, controls and responsibilities regarding access must be documented in order to comply with the intent of the Federal Information Security Management Act of 2002 for standards and guidelines on security and privacy.

- The System owner is responsible for ensuring that access to information and data is restricted to authorized personnel. Usually, a user is only given access to certain information that is needed to perform an official function. Care should be given to avoid "open Systems" where all information can be viewed by all users. System administrators may be afforded greater access – i.e. to all of the data – depending upon the System and/or application. However, restrict access when users do not need to have access to all the data.

- When a contract provides for the operation of a System on behalf of FHFA, the Privacy Act requirements must be applied to such a System. Contact the Contracting Officer or

Contracting Officer's Representative to determine whether the contract contains the Privacy Act clause and the requirements thereunder.

- The Security Assessment and Authorization (SA&A) process requires a System security plan that identifies the technical controls associated with identification and authentication of users. Certain laws and regulations require monitoring of Systems to ensure that only authorized users can access the System for authorized reasons. In doing so, consider what controls are in place to ensure that only those authorized to monitor the System can in fact monitor use of the System. For example, business rules, internal instructions, and posting Privacy Warning Notices address access controls and violations for unauthorized monitoring. System Owners are responsible for ensuring that no unauthorized monitoring is occurring.

- The IT Security Plan describes the practice of applying logical access controls. Logical access controls are System-based means by which the ability to access a System is either explicitly enabled or restricted. System Owners are responsible for ensuring that no unauthorized access is occurring.

- The IT Security Plan describes the practice of audit trails. An audit trail maintains a record of System activity and user activity including invalid logon attempts, access to data and monitoring. The SA&A process requires a System security plan outlining the implementation of the technical controls associated with identification and authentication.

- Every System/application/process that uses data must have controls in place to prevent the misuse of the data by those having access to the data. For instance, in computerized Systems, the Security Information Record (SIR) is part of the Core Storage Terminal Table. The SIR is the automated tool that identifies and authenticates an individual for the System and is transparent to the user.

- All employees, including contractors, have requirements for protecting information in Privacy Act Systems. Describe the controls in place, including any privacy and security awareness controls such as training materials, to protect the information.

PIA FORM

Overview

Provide an overview of the System and address the following:

- The System name and the division/office that owns the System;
- The purpose of the program, System, or technology and how it relates to the agency's mission; and
- A general description of the information in the System.

System Owner(s)			
Name	**E-mail**	**Division/Office**	**Office or Mobile Phone Number**
Lindsay Rosenquist Burns	Lindsay.Rosenquist@fhfa.gov	DCOR/OCO	202-649-3408
Roshni Uttamsingh	Roshni.Uttamsingh@fhfa.gov	DCOR/OCO	202-649-3293

System Overview: Briefly describe the purpose of the program, System, or technology, and the information in the System, and how it relates to the agency's mission.

The purpose of the OCO STAR system is to:

1) List and track all issues submitted by Fannie Mae, Freddie Mac and Common Securitization Solutions (collectively referred to as the " GSEs" for purpose of this document) that require FHFA's review or action as Conservator;

2) Assist FHFA with generating reports for Conservatorship Committee (CC) meetings, FHFA's Office of Inspector General (OIG) and Congress as required;

3) Collect information to evaluate prospective senior-level employees and board candidates for the GSEs and their affiliates, as part of FHFA's statutory authority to oversee the prudential operations of each GSE; and

4) Serve as a records management system for all decisions and directives issued by FHFA.

Section 1.0 Characterization of the Information

The following questions define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, System, or technology being developed. The questions address all information collected, with more emphasis provided on the collection of PII, such as name, address, social security number, date of birth, financial information, etc.

#	Question	Response
1.1	What information is being collected, used, disseminated, or maintained in the System?	OCO STAR collects the name and contact information (e.g. business email address and telephone number) for employees from the GSEs. OCO STAR also collects the following information for prospective senior-level employees, executives, and board candidates for the GSEs: • name; contact information (*e.g.*,

		business and home addresses, business and personal email addresses, business and personal telephone numbers); • educational credentials; and • work history. This information may also include independent contractor engagements, professional compensation history, investment holdings information, and criminal background checks for current and prospective senior-level employees, executives and board candidates, along with their family members.
1.2	What or who are the sources of the information in the System?	FHFA receives the information in OCO STAR from the GSEs.
1.3	For what purpose is the information being collected, used, disseminated, or maintained?	The purpose of this information collection is to: 1) List and track all issues submitted by the GSEs that require FHFA's review or action as Conservator; 2) Assist FHFA with generating reports for CC meetings, FHFA's OIG and Congress as required; 3) Collect information to evaluate prospective senior-level employees and board candidates for the GSEs and their affiliates, as part of FHFA's statutory authority to oversee the prudential operations of each GSE; and 4) Serve as a records management system for all decisions and directives issued by FHFA.

1.4	How is the information provided to FHFA?	The information in OCO STAR is provided to FHFA from the GSEs.
1.5	Given the amount and type of information collected, what are the risks to an individual's privacy that are associated with collection of the data? Explain in detail how the loss, or compromise of the information will/can affect an individual's privacy.	OCO STAR collects the name, contact information and financial information for private individuals. A loss of this information could compromise the personal privacy of the individuals who are the subject of the leak. To mitigate this risk, access to OCO STAR and the information therein is limited to those who have a need-to-know in the performance of their official duties.
1.6	Are Social Security Numbers (SSNs) are being collected or used in the system?	No, SSNs are not being collected or used in OCO STAR.
1.7	If SSNs are collected or used in the system, 1) describe in detail the business justification for collecting or using SSNs; 2) the consequences if SSNs are not collected or used, and 3) how the SSNs will be protected while in use, in transit and in storage.	N/A.

Section 2.0 Uses of the Information

The following questions delineate the use of information and the accuracy of the data being used.

#	Question	Response
2.1	How will the information be used and for what purpose?	OCO STAR will be used to: 1) List and track all issues submitted by the GSEs that require FHFA's review or action as Conservator; 2)Assist FHFA with generating reports for Conservatorship Committee (CC) meetings, FHFA's Office of Inspector General (IG) and Congress as required; 3) Collect information to evaluate prospective senior-level employees and board candidates for the GSEs and their affiliates, as part of FHFA's statutory authority to oversee the prudential operations of each GSE; and 4)Serve as a records management system for all decisions and directives issued by FHFA.
2.2	Describe any types of controls or safeguards in place to ensure that information is only used in the manner for which it was collected.	To ensure that information is only used in the manner for which is collected, access to OCO STAR and the information therein is limited to those individuals who have a need-to-know in the performance of their official duties.

Section 3.0 Retention

The following questions outline how long information will be retained after the initial collection.

#	Question	Response
3.1	How long is the information retained?	The information in OCO STAR will be retained permanently.
3.2	Has a retention schedule been approved by FHFA's Records Management Office and NARA? If yes, provide the corresponding GRS or FHFA specific Records Schedule number.	Yes, a retention schedule has been approved. The records will be retained pursuant to Item 3.2 of FHFA's Comprehensive Record Schedule. The NARA Authority for

		this Records Schedule is N1-543-11-1, as approved on 01/11/2013.
3.3	Discuss the risks associated with the length of time data is retained and how those risks are mitigated.	There are minimal risks associated with the length of time the data is retained. Access to OCO STAR and the information therein is continuously limited to those who have a need-to-know in the performance of their official duties.

Section 4.0 Notice, Access, Redress and Correction

The following questions are directed at notice to the individual, the individual's right to consent to uses of the information, the individual's right to decline to provide information, and an individual's ability to ensure the accuracy of the information collected about them.

#	Question	Response
4.1	Has a System of Record Notice (SORN) been created? If so, provide the SORN name and number. If one has not, and one is required, provide the name of the SORN and the expected publication date in the Federal Register.	There is not a SORN in place for this information collection yet. FHFA anticipates publishing the Regulated Entity Prospective Employee Directory SORN on 6/24/2022.
4.2	Was notice provided to the individual prior to collection of information? If so, what type of notice was provided?	N/A. The information that is collected in OCO STAR is provided to FHFA from the GSEs.
4.3	Do individuals have the opportunity and/or right to decline to provide information? What are the consequences if an individual declines to provide the information?	N/A. FHFA has a statutory right to obtain the information contained in OCO STAR in carrying out the Director's duty to oversee the prudential operations of the GSEs pursuant to 12 CFR § 1200.2 and 12 USC § 4513(a)(2)(B).

#	Question	Response
4.4	What are the procedures that allow individuals to gain access to their information?	Individuals may submit a Privacy Act request to FHFA's Privacy Act Officer per 12 CFR § 1204.3(b).
4.5	What are the procedures for correcting inaccurate or erroneous information?	Individuals may submit a request to amend or correct records to FHFA's Privacy Act Officer per 12 CFR § 1204.3(d).

Section 5.0 Sharing and Disclosure

The following questions define the content, scope, and authority for information sharing.

#	Question	Response
5.1	With which internal organization(s) is the information shared? What information is shared and for what purpose?	The information in OCO STAR is shared internally with the Office of General Counsel (OGC), Division of Bank Regulation (DBR), Division of Conservatorship Oversight and Readiness (DCOR) and Office of the Director (ODO). The information that will be shared consists of: 1) Documents provided to FHFA from the GSEs that require FHFA's review or action as Conservator; 2) Documents provided to FHFA from the GSEs to generate reports for CC meetings, FHFA's OIG and Congress as required; and 3) Documents provided to FHFA from the GSEs in order to evaluate prospective senior-level employees and board candidates for the GSEs and their affiliates. The purpose of sharing this information is to assist the Director in overseeing the prudential operations of the GSEs pursuant to 12 CFR § 1200.2 and 12 USC § 4513(a)(2)(B).
5.2	With which external organization(s) is the information shared? What information is shared, and for what purpose? External organization(s) include Federal, state and local government, and the private sector.	There is not one specific external organization with which the information will be shared. Information in OCO STAR may be shared externally for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to the audit or oversight function.

5.3	Is the sharing of PII outside the agency compatible with the original information collection? If so, is it covered by an appropriate routine use in a SORN? Describe such use. If not, describe the legal authority that permits PII to be shared outside of FHFA.	Yes, the sharing of PII outside the agency is compatible with the original information collection. FHFA anticipates publishing the Regulated Entity Prospective Employee Directory SORN on 6/24/2022. This SORN will include FHFA's routine uses for the sharing of PII in OCO STAR outside the agency. 5 USC 552a(b)(1)-(12) is FHFA's legal authority to share this information externally.
5.4	Given the external sharing, explain the privacy risks to the individual and describe how those risks are mitigated.	There are minimal risks associated with the external sharing of PII in OCO STAR. Access to OCO STAR and the information therein is continuously limited to those who have a need-to-know in the performance of their official duties. Furthermore, all information in OCO STAR that is shared externally will be aggregated to the maximum extent possible, to limit any specific individual being identifiable.

Section 6.0 Technical Access and Security

The following questions describe technical safeguards and security measures.

#	Question	Response
6.1	What procedures are in place to determine which users may access the System? Are these procedures documented in writing?	GSE employees can only access information in OCO STAR that has been submitted by their GSE employer. Access to OCO STAR and the information therein is limited to those who have a need-to-know in the performance of their official duties. This access is in alignment with FHFA's *Use and Protection of PII* policy.

6.2	Will non-FHFA personnel (e.g. contractor personnel, regulated entity personnel) have access to the System and information contained therein? If yes, how will they gain access to the System? How will the agency control their access and use of information? Are there procedures documented in writing?	Yes, non-FHFA personnel from the GSEs have access to OCO STAR via FHFA's extranet; however, GSE employees can only access information in OCO STAR that has been submitted by their GSE employer. System Owners control who may access OCO STAR and what information is accessible therein.
6.3	Describe the type and frequency of training that is provided to users either generally or specifically that is relevant to the program or System?	All FHFA employees are required to undergo annual privacy training for use of FHFA systems. GSE personnel are not required to take this annual training, since their access to OCO STAR is restricted to information submitted by their GSE employer.
6.4	Describe the technical/administrative safeguards in place to protect the data?	Access to OCO STAR and the information therein is restricted to FHFA employees with a need-to-know in the performance of their official duties and GSE employees who upload information into OCO STAR. Additionally, access to OCO STAR is granted and limited by the System Owners.
6.5	What auditing measures are in place to protect the data? Who reviews these measures and how frequently are they reviewed?	Access to OCO STAR and the information therein is restricted to FHFA employees with a need-to-know in the performance of their official duties and GSE employees who upload information into OCO STAR. System Owners conduct a weekly audit to review the list of individuals who accessed OCO STAR the previous week.

6.6	Has a SA&A been completed for the System or Systems supporting the program? If so, provide the date the last SA&A was completed. If not, and one is required, provided the expected completion date of the SA&A.	Yes, the SA&A for OCO STAR was completed on 7/26/21.
6.7	Has an Authority to Operate (ATO) been issued for this System? If so, what date was it issued, and for how long was it issued? If not, when do you anticipate such ATO being issued?	Yes, an ATO for OCO STAR was issued on 9/30/21.

Signatures

LINDSAY ROSENQUIST BURNS

Digitally signed by LINDSAY ROSENQUIST BURNS
Date: 2022.06.17 09:41:52 -04'00'

System Owner
Lindsay Rosenquist Burns

RALPH MOSIOS

Digitally signed by RALPH MOSIOS
Date: 2022.06.29 11:32:42 -04'00'

Chief Information Security Officer
Ralph Mosios

TASHA COOPER

Digitally signed by TASHA COOPER
Date: 2022.06.15 22:54:25 -04'00'

Senior Agency Official for Privacy
Tasha L. Cooper